

Regulamin obowiązuje od:

1 grudnia 2017 r. – w przypadku umów zawartych do 30 listopada 2017 r.

Od dnia zawarcia umowy – w przypadku umów zawartych od 1 grudnia 2017 r.



Regulamin korzystania z Kanałów Elektronicznych dla Klientów Indywidualnych

POSTANOWIENIA OGÓLNE

§1

1. Niniejszy Regulamin korzystania z Kanałów Elektronicznych dla Klientów Indywidualnych określa zasady i warunki udostępniania informacji o produktach Użytkownika oraz składania dyspozycji za pośrednictwem Kanałów Elektronicznych.
2. Regulamin jest załącznikiem do Umowy o świadczenie usług oferowanych przez Bank dla Osoby fizycznej i stanowi jej integralną część.
3. O ile w Regulaminie nie wskazano inaczej, to postanowienia Regulaminu nie mają zastosowania do umów zawartych z T-Mobile Usługi Bankowe i usług świadczonych poprzez T-Mobile Usługi Bankowe.

§2

Użyte w dalszej części Regulaminu pojęcia oznaczają:

Aktywacja systemu Bankowości Internetowej i Bankowości Mobilnej – szereg czynności wykonywanych przez Użytkownika w Bankowości Internetowej i Bankowości Mobilnej po zainstalowaniu Aplikacji Mobilnej, mających na celu zdefiniowanie PINu autoryzacyjnego używanego do autoryzacji transakcji w Aplikacji Mobilnej. Szczegółowa Instrukcja aktywacji została umieszczona na stronach internetowych Banku;

Aplikacja Mobilna – oprogramowanie zainstalowane na urządzeniu mobilnym takim jak smartfony, tablety i palmtopy, służące do obsługi Bankowości Mobilnej. Aplikacja Mobilna może być dostępna w różnych wersjach i pod różnymi nazwami handlowymi, które mogą różnić się między sobą wymogami technicznymi oraz funkcjonalnościami. Lista udostępnianych aplikacji mobilnych oraz ich zakres funkcjonalny, w tym rodzaje dyspozycji, jakie mogą zostać złożone przy ich pomocy znajdują się na stronie internetowej Banku;

Aplikacja HAIZ – aplikacja o nazwie HAIZ dostępna na urządzeniach mobilnych, umożliwiająca między innymi korespondowanie między Użytkownikami HAIZ oraz składanie określonych dyspozycji dotyczących transakcji finansowych (zwanych dalej Usługami finansowymi);

Bank – Alior Bank Spółka Akcyjna z siedzibą w Warszawie;

Bankowość Internetowa – usługa zapewniająca dostęp do informacji o Produktach Użytkownika oraz możliwość składania dyspozycji z wykorzystaniem sieci Internet i komputera wyposażonego w przeglądarkę internetową. Bankowość Internetowa Mobilna może być dostępna w różnych wersjach i pod różnymi nazwami handlowymi, które mogą się różnić między sobą wymogami technicznymi oraz funkcjonalnościami. Lista udostępnianych systemów oraz ich zakres funkcjonalny, w tym rodzaje dyspozycji, jakie mogą zostać złożone przy ich pomocy znajdują się na stronie internetowej Banku;

Bankowość Mobilna – usługa zapewniająca dostęp do informacji o Produktach Użytkownika oraz możliwość składania dyspozycji z wykorzystaniem urządzeń mobilnych takich jak palmtopy, tablety i telefony komórkowe z dostępem do Internetu, za pomocą przeglądarek internetowych lub Aplikacji Mobilnej;

Bankowość Telefoniczna – usługa zapewniająca dostęp do informacji o Produktach Użytkownika oraz możliwość składania dyspozycji przy użyciu telefonu z wybieraniem tonowym (może zostać naliczona opłata za połączenie zgodnie z taryfą operatora);

Biometria – metoda identyfikacji Użytkownika, polegająca na identyfikacji indywidualnych cech fizycznych Klienta, polegająca na porównaniu ich ze wzorcem przechowywanym w systemie informatycznym producenta urządzenia na którym zainstalowana jest Aplikacja Mobilna.

Biuro Maklerskie – wydzielona jednostka organizacyjna Banku odpowiedzialna za świadczenie przez Bank usług maklerskich;

Contact Center – jednostka Banku lub Biura Maklerskiego, świadcząca telefoniczną obsługę dla aktualnych oraz potencjalnych Użytkowników, w zakresie informacyjnym, sprzedażowym oraz transakcyjnym;

Dyspozycja – oświadczenie woli złożone przez Użytkownika za pośrednictwem Kanałów Elektronicznych i autoryzowane w sposób właściwy dla danego kanału;

Fraza Weryfikacyjna (hasło do zwrotnej weryfikacji Banku) – słowo, zwrot lub ciąg znaków ustalone przez Użytkownika, wykorzystywane do identyfikacji pracownika Banku kontaktującego się telefonicznie z Użytkownikiem w sytuacji, gdy kontakt inicjowany jest przez Bank;

Hasło Startowe – ciąg cyfr przesyłany Użytkownikowi na Telefon do Kodów autoryzacyjnych w formie wiadomości tekstowej lub ustalany przez Użytkownika w IVR, służący do aktywacji Bankowości Internetowej;

Hasło Dostępu – ciąg znaków, ustalany samodzielnie przez Użytkownika w Bankowości Internetowej, który użyty wraz z Identyfikatorem umożliwia dostęp do Bankowości Internetowej oraz do Bankowości Mobilnej;

Identyfikator (numer Kartoteki Klienta, CIF, alias) – unikalny numer nadany Użytkownikowi przez Bank, z którym jednoznacznie związane są dane osobowe i adresowe, służący m.in. do identyfikacji podczas korzystania z Kanałów Elektronicznych;

Identyfikacja biometryczna – metoda logowania do Aplikacji Mobilnej umożliwiająca rozpoznawanie tożsamości na podstawie indywidualnych cech fizycznych Klienta (min. takich jak odcisk palca lub jego wizerunek), udostępniana na urządzeniu mobilnym przez jego producenta i wymagająca uprzedniego włączenia stosownych funkcjonalności oraz ich rejestracji (metoda dostępna dla wybranych urządzeń zgodnie z aktualnymi informacjami na stronie internetowej Banku).

IVR – usługa zapewniająca całodobowy, automatyczny dostęp do informacji o Produktach Użytkownika przy użyciu telefonu z wybieraniem tonowym;

Kanały Elektroniczne – Bankowość Internetowa, Bankowość Telefoniczna, Bankowość Mobilna, IVR, Aplikacja HAIZ;

Kod autoryzacyjny – kod w formie wiadomości tekstowej przesyłany na Telefon zdefiniowany przez Użytkownika do autoryzacji zleceń, służący do autoryzacji Dyspozycji składanych przez Użytkownika w ramach Bankowości Internetowej lub Bankowości Mobilnej przy pomocy przeglądarek internetowych;

PIN autoryzacyjny – ciąg cyfr ustalany przez Użytkownika w sposób poufny podczas aktywacji Aplikacji Mobilnej, służący do autoryzacji Dyspozycji zleczanych przy pomocy Aplikacji Mobilnej;

Placówka Banku – jednostka organizacyjna Banku wykonująca czynności bankowe;

Połącz punkty – ciąg gestów na ekranie dotykowym, ustalany samodzielnie przez Użytkownika w Aplikacji Mobilnej, który użyty wraz z Identyfikatorem umożliwia dostęp do Aplikacji Mobilnej;

Powiadomienia finansowe – usługa umożliwiająca przesyłanie Użytkownikowi, informacji na temat Produktów użytkownika oraz usług świadczonych przez Bank lub Biuro Maklerskie; powiadomienia są przesyłane w postaci jawnej (nieszyfrowanej);

Produkt – rachunek lub usługa oferowana przez Bank lub Biuro Maklerskie świadczona na podstawie odpowiedniej umowy i regulaminu;

Przelew telefoniczny – typ płatności krajowej w PLN umożliwiający zlecenie i otrzymywanie przelewów przez Użytkownika, którego tożsamość identyfikowana jest przez numer telefonu komórkowego, przy czym korzystanie z tej funkcjonalności wymaga uprzedniej rejestracji tzw. Aliasu tj. powiązania swojego numeru telefonu i rachunku, na który przelewy mają być księgowane. Użytkownik definiując alias BLIK wyraża zgodę na przekazanie przez Bank numeru rachunku bankowego innym uczestnikom transakcji.

Telefon do Kodów autoryzacyjnych – podany przez Użytkownika numer telefonu komórkowego, na który przesyłane jest Hasło Startowe oraz Kody autoryzacyjne

Tele PIN – ciąg cyfr ustalany przez Użytkownika w sposób poufny podczas aktywacji Bankowości Telefonicznej, służący do weryfikacji Użytkownika w ramach tej usługi;

T-Mobile Usługi Bankowe – oddział Alior Banku S.A.;

Transakcje kartą mobilną (NFC/HCE) – typ płatności bezgotówkowych realizowanych za pomocą Aplikacji Mobilnej oraz ztokenizowanej karty płatniczej;

Umowa – Umowa ramowa o świadczenie usług oferowanych przez Bank dla Osoby Fizycznej, zawarta pomiędzy Bankiem i osobą fizyczną, na podstawie której możliwe jest korzystanie z Kanałów Elektronicznych;

Użytkownik – Osoba fizyczna, która zawarła Umowę i jest uprawniona do składania Dyspozycji za pośrednictwem Kanałów Elektronicznych;

Użytkownik HAIZ – Osoba fizyczna, która zawarła Umowę i jest uprawniona do składania Dyspozycji za pośrednictwem Kanałów Elektronicznych korzystająca z aplikacji HAIZ.

APLIKACJA HAIZ

§3

Szczegóły dotyczące korzystania oraz zakresu usług, w tym uruchomienia Aplikacji HAIZ zostały określone w Regulaminie Aplikacji oraz Usług HAIZ, dostępnym na stronie internetowej Banku oraz w Placówkach Banku.

WARUNKI UDOSTĘPNIANIA KANAŁÓW ELEKTRONICZNYCH

§4

Kanały Elektroniczne, z wyłączeniem Aplikacji HAIZ, są udostępniane po spełnieniu łącznie następujących warunków:

- Zawarcia Umowy przez Użytkownika lub jego przedstawiciela ustawowego:
 - osobiście, w Placówce Banku,
 - korespondencyjnie,
 - w inny wskazany przez Bank sposób zgodny z obowiązującymi przepisami prawa.
- Dokonania przez Użytkownika aktywacji wybranego Kanału Elektronicznego poprzez podanie Identyfikatora oraz:
 - Hasła Startowego, w przypadku Bankowości Internetowej,
 - przeprowadzenie pozytywnej weryfikacji danych osobowych podczas rozmowy z konsultantem Contact Center, w przypadku Bankowości Telefonicznej.
- Wybrania sposobu logowania do Bankowości Internetowej oraz Mobilnej:
 - Hasło Dostępu w Bankowości Internetowej oraz Mobilnej – w przypadku obsługi przy pomocy przeglądarek internetowych,
 - opcjonalnie: PIN lub Identyfikacja biometryczna (od momentu udostępnienia funkcjonalności).

§5

- W przypadku osoby małoletniej, która nie ukończyła 13. roku życia, aktywacji Kanałów Elektronicznych, z wyłączeniem Aplikacji HAIZ, może dokonać wyłącznie przedstawiciel ustawowy. Hasło Startowe oraz Kody autoryzacyjne przesyłane są na należący do przedstawiciela ustawowego Telefon do Kodów autoryzacyjnych.
- W przypadku osoby małoletniej, która ukończyła 13. rok życia, aktywacji Kanałów Elektronicznych, z wyłączeniem Aplikacji HAIZ, może dokonać osoba małoletnia lub jej przedstawiciel ustawowy, zgodnie z decyzją przedstawiciela wyrażoną podczas zawierania Umowy. Hasło Startowe oraz Kody autoryzacyjne przesyłane są odpowiednio na Telefon do Kodów autoryzacyjnych osoby małoletniej lub Telefon do Kodów autoryzacyjnych przedstawiciela ustawowego.
- W przypadku osób małoletnich, korzystanie z Aplikacji HAIZ określa Regulamin Aplikacji oraz Usług HAIZ.

§6

Bankowość Internetowa lub Bankowość Mobilna mogą być aktywowane niezależnie od siebie, w dowolnej kolejności.

§7

Po dokonaniu aktywacji Kanałów Elektronicznych, Użytkownik uzyskuje dostęp do wybranych Produktów, w tym otwartych w przyszłości.

ZAKRES USŁUG KANAŁÓW ELEKTRONICZNYCH

§8

Kanały Elektroniczne umożliwiają Użytkownikowi zarządzanie środkami finansowymi, uzyskiwanie informacji o posiadanych Produktach oraz zawieranie umów o wybrane Produkty. Szczegółowy zakres dostępnych informacji i lista Dyspozycji możliwych do wykonania w poszczególnych Kanałach Elektronicznych publikowane są na stronach internetowych Banku, Biura Maklerskiego oraz dostępne w Placówkach Banku i u konsultantów Contact Center. Zasady korzystania z Transakcji kartą mobilną zostały określone w Regulaminie kart płatniczych, podczas gdy do usługi Przelewów na telefon stosuje się Regulamin rachunków oszczędnościowo-rozliczeniowych, w zakresie dotyczącym Usługi BLIK.

§9

Bank może zmienić zakres informacji i Dyspozycji dostępnych za pośrednictwem Kanałów Elektronicznych w przypadku wprowadzania nowych lub zmiany powszechnie obowiązujących przepisów prawa lub zmian w ofercie Banku.

§10

- Bank udostępnia Użytkownikom usługę Powiadomień finansowych będących potwierdzeniem zdarzenia na rachunku Użytkownika.
- Powiadomienia finansowe mogą być przesyłane:
 - jako komunikat SMS,
 - jako wiadomość email,
 - poprzez Bankowość Internetową,
 - jako mobilne powiadomienie PUSH dla Bankowości Mobilnej (od momentu udostępnienia funkcjonalności).
- Zakres powiadomień definiowany jest przez Użytkownika poprzez formularz dostępny w Bankowości Internetowej lub Mobilnej z zastrzeżeniem ust. 5.
- Powiadomienia finansowe wysyłane są niezwłocznie po wystąpieniu zdarzenia, z zastrzeżeniem, że w godzinach nocnych wysyłane są jedynie powiadomienia krytyczne (informacje o godzinach i zakresie powiadomień zostały podane w Bankowości Internetowej).
- Bank ma prawo wysyłać dodatkowe powiadomienia SMS z informacją o zdarzeniach na rachunku. Za powiadomienia takie nie jest pobierana opłata.

REALIZACJA DYSPOZYCJI I ZASADY KORZYSTANIA Z KANAŁÓW ELEKTRONICZNYCH

§11

Dyspozycje za pośrednictwem Kanałów Elektronicznych mogą być składane codziennie, w ciągu całej doby, za wyjątkiem ogłoszonych wcześniej przerw konserwacyjnych.

§12

Aktualne informacje o trybie i warunkach realizacji Dyspozycji są publikowane na stronie internetowej Banku i Biura Maklerskiego.

§13

1. Dyspozycje składane przez Bankowość Internetową lub Bankowość Mobilną przy pomocy przeglądarek internetowych, mogą wymagać autoryzacji za pomocą Kodu autoryzacyjnego.
2. Dyspozycje składane przez Bankowość Internetową lub Bankowość Mobilną mogą wymagać autoryzacji za pomocą PINu autoryzacyjnego lub kodu SMS.
3. Dyspozycje składane przez Bankowość Telefoniczną mogą wymagać autoryzacji za pomocą Kodu autoryzacyjnego.
4. Użytkownik nie może podważać autentyczności prawidłowo zautoryzowanej Dyspozycji.

§14

1. Dyspozycja z bieżącą datą realizacji, prawidłowo zautoryzowana, nie może być anulowana.
2. Zapisy ust. 1 nie wykluczają możliwości złożenia Dyspozycji anulowania zlecenia w ramach świadczonych usług maklerskich na zasadach określonych w regulaminie świadczenia danej usługi maklerskiej.

§15

1. Dane niezbędne do prawidłowej realizacji Dyspozycji powinny być podane zgodnie z opisem pól występujących w formularzu Dyspozycji.
2. Przed dokonaniem autoryzacji, Użytkownik powinien upewnić się, że Dyspozycje są jednoznaczne i zgodne z jego intencją, w tym w szczególności te, które są zlecane na podstawie zdjęć faktur lub rachunków wykonywanych przez urządzenie mobilne.

§16

1. Bank rejestruje i przechowuje na nośnikach elektronicznych wszystkie rozmowy telefoniczne prowadzone w ramach Contact Center.
2. Użytkownik wyraża zgodę na rejestrowanie tych rozmów.
3. W przypadku braku zgody Użytkownika lub awarii urządzenia nagrywającego, Bank ma prawo odmówić przyjęcia Dyspozycji drogą telefoniczną.
4. W razie wątpliwości co do treści złożonej Dyspozycji, nagrania rozmów są rozstrzygające i mogą być wykorzystane w postępowaniu reklamacyjnym oraz dla celów dowodowych.

§17

Dyspozycje dotyczące obsługi zleceń stałych wykonywanych z rachunków bankowych oraz odwoływania przelewów z odroczoną datą realizacji są przyjmowane najpóźniej na jeden dzień roboczy przed datą realizacji Dyspozycji.

§18

Jeśli zachodzi uzasadnione podejrzenie co do autentyczności złożonej Dyspozycji, Bank może wstrzymać jej realizację do momentu wyjaśnienia wątpliwości lub odmówić jej wykonania.

§19

1. Maksymalna kwota, na jaką można zlecić przelew poprzez Bankowość Internetową i Bankowość Mobilną, publikowana jest na stronie internetowej Banku i Biura Maklerskiego, przy czym limity te mogą być różne dla różnych wersji Bankowości Internetowej i/lub Aplikacji Mobilnej oraz dla różnych typów Dyspozycji. Przelewy przekraczające wskazaną kwotę nie są realizowane. W przypadku przelewów wykonywanych w walutach obcych, maksymalna kwota wyznaczana jest poprzez przeliczenie na PLN kwoty, o której mowa w ust. 1. Przeliczenie realizowane jest według aktualnego kursu kupna/sprzedaży dewiz obowiązującego w Banku w chwili zlecenia przelewu.
2. Limit, o którym mowa w ust.1, obowiązywać będzie od dnia 1 sierpnia 2017 r.
3. Ograniczenie, o którym mowa w ust. 1, 2 i 3 nie ma zastosowania do przelewów zlecanych z wykorzystaniem szablonu płatności zdefiniowanego w Placówce Banku oraz do przelewów własnych. Przelewy realizowane poprzez Bankowość Telefoniczną podlegają odrębnym limitom kwotowym. Informacje o maksymalnej kwocie przelewu realizowanego poprzez Contact Center zamieszczone są na stronach internetowych Banku oraz dostępne u konsultantów.

ZASADY BEZPIECZEŃSTWA

§20

Bank, świadcząc usługi na podstawie niniejszego Regulaminu, zobowiązuje się do zapewnienia Użytkownikowi bezpieczeństwa wykonywania Dyspozycji, z zachowaniem należytej staranności oraz przy wykorzystaniu właściwych rozwiązań technicznych.

§21

Użytkownik nie może dostarczać danych o charakterze bezprawnym i zobowiązany jest stosować się do zaleceń Banku w zakresie zasad bezpieczeństwa podczas korzystania z Kanałów Elektronicznych; w szczególności Użytkownik powinien z należytą starannością chronić dane wykorzystywane do logowania w Kanałach Elektronicznych (Identyfikator, w tym również identyfikator biometryczny, hasła, PIN-y) oraz telefon komórkowy, którego numer został podany w Banku jako Telefon do autoryzacji zleceń za pośrednictwem Kodów autoryzacyjnych oraz zobowiązany jest każdorazowo do dokładnego zapoznania się z treścią komunikatu SMS zawierającego poszczególny Kod autoryzacyjny, w celu zweryfikowania jego zgodności ze złożoną przez Użytkownika Dyspozycją. Użytkownik jest zobowiązany również z należytą starannością chronić urządzenie z zainstalowaną Aplikacją Mobilną.

§22

Użytkownik zobowiązany jest do niezwłocznego poinformowania Banku oraz niezwłocznego dokonania zmiany hasła lub zablokowania Kanałów Elektronicznych w przypadku:

1. ujawnienia lub udostępnienia osobom trzecim danych logowania lub podejrzenia takiego zdarzenia,
2. nieautoryzowanego użycia Kanałów Elektronicznych,
3. wykrycia nieautoryzowanych transakcji i operacji na rachunkach klienta,
4. utraty lub kradzieży danych logowania,
5. zmiany, utraty lub udostępnieniu osobom trzecim numeru telefonu używanego do kontaktu z Bankiem, w szczególności używanego do autoryzacji transakcji
6. utraty urządzenia mobilnego umożliwiającego korzystanie z bankowości mobilnej.

§23

Bank zastrzega sobie prawo wprowadzenia dodatkowych ograniczeń i zabezpieczeń w stosunku do dyspozycji składanych w Kanałach Elektronicznych, w przypadku wystąpienia ważnych okoliczności uzasadniających wprowadzenie takich środków.

§24

1. Szczegółowe informacje dotyczące zasad bezpiecznego korzystania z Kanałów Elektronicznych oraz ryzyk związanych z korzystaniem z nich, wskazane zostały w §25 oraz zamieszczone są na stronach internetowych Banku, a także udzielane przez konsultantów Contact Center.
2. Użytkownik zobowiązany jest przestrzegać zasad bezpiecznego korzystania z Kanałów Elektronicznych, a w przypadku ich nieprzestrzegania działa na własne ryzyko i ponosi odpowiedzialność za skutki takiego zaniechania.

§25

Użytkownik przyjmuje do wiadomości, że elektroniczny dostęp do systemów Bankowości Internetowej, Mobilnej i Telefonicznej, wiąże się z ryzykami – w szczególności w przypadku nieprzestrzegania zasad bezpieczeństwa określonych przez Bank. Do tych ryzyk należą przede wszystkim:

1. Ryzyko zagubienia lub kradzieży przez osoby nieuprawnione danych lub urządzeń:
 - a. służących do zalogowania do systemu (np. identyfikator, tym również identyfikator biometryczny/hasło lub PIN do Aplikacji Mobilnej),
 - b. służących do zatwierdzania transakcji (np. urządzenia mobilnego z zainstalowaną aplikacją).
2. Ryzyko wystąpienia ataków socjotechnicznych, w których osoby trzecie będą – podszywając się pod Bank – nakłaniały Użytkownika do zatwierdzania operacji (np. fałszywa informacja o konieczności wykupienia transakcji).
3. Ryzyko nieświadomego zatwierdzenia przez Użytkownika niezamierzonych zleceń (np. bez zapoznania się z operacją opisaną w Kodzie autoryzacyjnym).
4. Ryzyko wykorzystania, w trakcie korzystania z Kanałów Elektronicznych, urządzeń, nad którymi kontrolę w sposób zdalny lub fizyczny przejęły osoby trzecie (np. za pomocą złośliwego oprogramowania, takiego jak wirusy).
5. Konsekwencjami wystąpienia ww. ryzyk mogą być:
 - a. dostęp osób trzecich do danych Użytkownika dostępnych w Kanałach Elektronicznych,
 - b. możliwość realizacji transakcji przez osoby trzecie w imieniu Użytkownika – w tym finansowych (np. wykonywanie przelewów),
 - c. możliwość zatwierdzenia niechcianej transakcji przez Użytkownika.

§26

Podczas korzystania z Bankowości Internetowej oraz Bankowości Mobilnej, Bank zaleca używanie przeglądarek internetowych z listy referencyjnej umieszczonej na stronie internetowej Banku. Bank nie ponosi odpowiedzialności za ewentualne nieprawidłowości w funkcjonowaniu Bankowości Internetowej oraz Bankowości Mobilnej w przypadku używania przeglądarek spoza tej listy.

§27

Podstawowe zasady bezpieczeństwa w trakcie korzystania z Kanałów Elektronicznych:

1. Zawsze należy sprawdzać poprawność adresu logowania do Bankowości Internetowej (w zależności od dostępnej wersji: <https://aliorbank.pl/hades/do/Login> lub <https://system.aliorbank.pl/>). Przy logowaniu należy zwracać uwagę czy przeglądarka nie wyświetla ostrzeżeń związanych z certyfikatem bezpieczeństwa (należy wejść

w jego szczegóły) oraz na przedrostek HTTPS w adresie strony logowania, świadczący o szyfrowaniu połączenia ze stroną Systemu Bankowości Internetowej.

2. Należy uważnie czytać treść Kodów autoryzacyjnych. Przed potwierdzeniem operacji należy przeczytać dokładnie całą wiadomość SMS. Bank nigdy nie poprosi o potwierdzenie operacji, która nie została zlecona przez Użytkownika.
3. Bank zaleca regularne aktualizacje systemu operacyjnego oraz zainstalowanego na nim oprogramowania, w szczególności oprogramowania antywirusowego (wraz z bazą sygnatur wirusów) oraz wykorzystywanej przeglądarki internetowej.
4. Nie należy korzystać z niezaufanych urządzeń do logowania do Bankowości Internetowej (np. w kafejce internetowej) lub na komputerze, na którym zalogowany jest inny użytkownik - do tego celu nie należy również używać publicznych sieci Wi-Fi.
5. Należy zwrócić szczególną uwagę na ataki mające na celu namówienie do wykonania jakiejś akcji (np. kliknięcie w link, pobranie oprogramowania, podanie swoich danych), które są przesyłane w e-mailach, wiadomościach SMS/MMS, sieciach społecznościowych, komunikatorach lub są przekazywane telefonicznie.
6. Bank zaleca aby nie otwierać załączników ani nie używać odnośników z podejrzanych e-maili (np. z błędami, literówkami, nieskładną gramatyką; pochodzących z innego adresu niż oficjalny, które nie były oczekiwane itp.) oraz aby na te wiadomości nie odpowiadać. Fałszywe maile są najczęstszą przyczyną zarażenia komputerów niebezpiecznym, złośliwym oprogramowaniem.
7. Istotne dane (adres, numery PESEL, hasła, loginy i inne wrażliwe dane) powinny być należycie chronione. Niedopuszczalnym jest udostępnianie przez Użytkownika swoich danych niezaufanym podmiotom lub osobom. Należy chronić swoje dokumenty, a w razie ich zagubienia bądź kradzieży natychmiast je zastrzec. Należy pamiętać, że przejęcie danych przez przestępców może zostać przez nich wykorzystane do kradzieży tożsamości, danych lub środków.
8. Należy zwracać uwagę na informacje o nowych zagrożeniach – na stronach Banku regularnie pojawiają się informacje w jaki sposób je rozpoznać i jak się przed nimi ustrzec (w sekcji Nowe zagrożenia oraz poprzez banery informacyjne na stronie logowania).
9. Należy zwracać uwagę na treści znajdujące się na stronie logowania do Bankowości Internetowej. Jeśli proces logowania wygląda inaczej niż zwykle (np. trwa znacznie dłużej, pojawiają się nowe okienka, użytkownik jest proszony o potwierdzenie operacji kodem SMS przy logowaniu) należy niezwłocznie skontaktować się z Contact Center – może to świadczyć o tym, że komputer jest zarażony złośliwym oprogramowaniem.
10. Użytkownik ponosi pełną odpowiedzialność za operacje i czynności wykonane przez osoby, którym ujawnił poświadczenia logowania lub udostępnił urządzenie służące do uwierzytelnienia i/lub autoryzacji operacji w Kanale Elektronicznym oraz za czynności i operacje, do których doszło w wyniku naruszenia przez użytkownika postanowień niniejszego Regulaminu.
11. Użytkownik zobowiązuje się chronić dostęp do swojego urządzenia mobilnego i przyjmuje do wiadomości, że pozyskanie przez osoby trzecie próbek biometrycznych zarejestrowanych w Usłudze Identyfikacji Biometrycznej, może prowadzić do uzyskania przez te osoby nieuprawnionego dostępu do Aplikacji Mobilnej.
12. Użytkownik ponosi odpowiedzialność z tytułu umożliwienia osobom trzecim zarejestrowania przez nich swoich próbek biometrycznych w Usłudze Identyfikacji Biometrycznej na urządzeniu mobilnym, na którym jest zainstalowana Aplikacja Mobilna z włączoną funkcją Logowania Odciskiem Palca.
13. Użytkownik jest zobowiązany poinformować Bank w przypadku zmiany numeru telefonu komórkowego, w formie pisemnej lub przez elektroniczne kanały dostępu,

niezwłocznie po zaistnieniu sytuacji. Użytkownik narażony jest i ponosi odpowiedzialność za negatywne konsekwencje w przypadku braku aktualizacji tego numeru.

14. W przypadku pytań/wątpliwości dotyczących bezpieczeństwa usług Banku lub zgłoszenia zdarzenia związanego z bezpieczeństwem prosimy o kontakt z Contact Center lub dowolnym oddziałem Alior Banku.
15. W przypadku wątpliwości dotyczących autentyczności komunikatów bezpieczeństwa otrzymywanych drogą mailową lub innym kanałem, należy porównać je z informacjami znajdującymi się na stronach Banku w sekcji Bezpieczeństwo.

ZABLOKOWANIE I REZYGNACJA Z KANAŁÓW ELEKTRONICZNYCH

§28

1. Przez zablokowanie należy rozumieć brak możliwości korzystania przez Użytkownika z danego Kanału Elektronicznego.
2. Zablokowanie Bańkowości Internetowej oraz Zablokowanie Bankowości Mobilnej mogą nastąpić zarówno łącznie, jak i niezależnie od siebie.

§29

1. Zablokowanie każdego z Kanałów Elektronicznych, z wyłączeniem Aplikacji HAIZ, może zostać dokonane przez Użytkownika:
 - a. samodzielnie w Bankowości Internetowej,
 - b. w drodze Dyspozycji złożonej konsultantowi Contact Center,
 - c. w Placówce Banku,
 - d. w wyniku przekroczenia ustalonego dla danego Kanału Elektronicznego limitu błędnych prób logowania.
2. Zablokowanie każdego z Kanałów Elektronicznych może zostać dokonane przez Bank na podstawie analizy danych systemowych w przypadku:
 - a. zagrożenia przechwycenia danych dostępowych Użytkownika przez złośliwe oprogramowanie,
 - b. wykorzystywania danych dostępowych Użytkownika przez oprogramowanie automatycznie logujące się z dużą częstotliwością,
 - c. wykorzystywania systemów lub rachunków w sposób niezgodny z obowiązującymi przepisami prawa,
 - d. wykonywanie działań mogących zagrażać bezpieczeństwu systemu i danych w nim przetwarzanych,
 - e. podejrzenia przez Bank, że osoba trzecia weszła w posiadanie dostępu do Kanałów Elektronicznych Użytkownika,
 - f. braku aktywacji przez Użytkownika Kanału Elektronicznego w ciągu trzech miesięcy od podpisania Umowy.
3. Niezwłocznie po zablokowaniu Bank podejmie kontakt z Użytkownikiem celem wyjaśnienia sytuacji. Nie dotyczy to sytuacji opisanej w ust. 2 pkt f.

§30

Użytkownik może odblokować:

1. Bankowość Telefoniczną – w drodze Dyspozycji złożonej konsultantowi Contact Center, w Placówce Banku lub samodzielnie w Bankowości Internetowej, o ile kanał ten jest aktywny,
2. Bankowość Internetową i Mobilną – w Placówce Banku lub w drodze Dyspozycji złożonej konsultantowi Contact Center, o ile kanał ten jest aktywny.

§31

W przypadku rozwiązania Umowy, Bank dokonuje zablokowania Kanałów Elektronicznych.

§32

Bank ma prawo do czasowego wyłączenia Kanałów Elektronicznych, po uprzednim umieszczeniu stosownego komunikatu na stronach internetowych Banku.

REKLAMACJE

§33

1. Bank rozpatruje reklamacje niezwłocznie, nie później niż w terminie 30 dni od dnia otrzymania reklamacji. W szczególnie skomplikowanych przypadkach termin ten może zostać przedłużony, nie więcej jednak niż do 60 dni od dnia otrzymania reklamacji. O przyczynach opóźnienia, okolicznościach wymagających ustalenia oraz przewidywanym terminie rozpatrzenia reklamacji i udzielenia odpowiedzi Użytkownik zostanie poinformowany.
2. Użytkownik zobowiązany jest dostarczyć Bankowi wszelkie informacje oraz dokumentację dot. reklamacji i współpracować z Bankiem do czasu zakończenia rozpatrywania reklamacji.
3. Reklamacja może być zgłoszona:
 - a. bezpośrednio w Placówce Banku,
 - b. telefonicznie w Contact Center,
 - c. poprzez System Bankowości Internetowej (dla Użytkownika zalogowanego),
 - d. listownie – na adres korespondencyjny Banku.
4. Odpowiedź na reklamację może zostać udzielona:
 - a. listownie,
 - b. poprzez System Bankowości Internetowej (dla Użytkownika zalogowanego),
 - c. poprzez SMS,a także w uzasadnionych przypadkach, dodatkowo:
 - d. telefonicznie,
 - e. w placówce Banku.
5. Użytkownik niezadowolony ze sposobu rozpatrzenia reklamacji uprawniony jest do zwrócenia się w sprawie sporu dotyczącego relacji z Bankiem:
 - a. do Arbitra Bankowego – w trybie pozasądowego postępowania w celu rozwiązania sporu, o ile wartość przedmiotu sporu nie jest wyższa niż 8.000,00 PLN (szczegółowe informacje, w tym Regulamin Bankowego Arbitrażu Konsumenckiego, dostępne na stronie internetowej www.zbp.pl);
 - b. do Rzecznika Finansowego - w trybie skargowym lub pozasądowego postępowania w celu rozwiązywania sporu (szczegółowe informacje dostępne na stronie internetowej www.rf.gov.pl).

POSTANOWIENIA KOŃCOWE

§34

1. Za czynności związane z udostępnieniem i obsługą Kanałów Elektronicznych Bank pobiera opłaty i prowizje zgodnie z obowiązującą Taryfą Opłat i Prowizji Alior Banku S.A. dla Klientów Indywidualnych lub Biura Maklerskiego.
2. Zmiany opłat i prowizji mogą nastąpić w przypadku wystąpienia przynajmniej jednego z poniższych warunków:
 - a. zmiana wysokości płacy minimalnej oraz poziomu wskaźników publikowanych przez GUS: inflacji, przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw;
 - b. zmiany cen energii, połączeń telekomunikacyjnych, usług pocztowych, rozliczeń międzybankowych oraz stóp procentowych ustalanych przez Narodowy Bank Polski;

- c. zmiany cen usług i operacji, z których Bank korzysta przy wykonywaniu poszczególnych czynności bankowych i niebankowych;
 - d. zmiany zakresu lub formy świadczonych przez Bank usług (w tym zmiany lub dodania nowej funkcjonalności w zakresie obsługi danego produktu) w zakresie, w jakim te zmiany mają wpływ na koszty ponoszone przez Bank w związku z wykonywaniem umowy;
 - e. zmiany przepisów prawa regulujących produkty lub usługi oferowane przez Bank lub mających wpływ na wykonywanie umowy, w zakresie, w jakim te zmiany mają wpływ na koszty ponoszone przez Bank w związku z wykonywaniem umowy;
 - f. zmiany przepisów podatkowych i/lub zasad rachunkowości stosowanych przez Bank, w zakresie w jakim te zmiany mają wpływ na koszty ponoszone przez Bank w związku z wykonywaniem umowy;
 - g. zmiana lub wydanie nowych orzeczeń sądowych, orzeczeń organów administracji, zaleceń lub rekomendacji uprawnionych organów, w tym Komisji Nadzoru Finansowego – w zakresie mającym wpływ na koszty ponoszone przez Bank w związku z wykonywaniem umowy.
3. Zmiany stawek opłat i prowizji następują na zasadach i w wysokości określonych w Taryfie Opłat i Prowizji dla Klientów Indywidualnych
 4. Aktualna Taryfa Opłat i Prowizji dostępna jest na stronach internetowych Banku oraz w Placówkach Banku.

§35

1. Bank zastrzega sobie prawo do dokonania zmiany niniejszego Regulaminu, w przypadku wystąpienia przynajmniej jednej z poniższych przyczyn:
 - a. zmiana w zakresie funkcjonowania oferowanych przez Bank produktów i usług; w tym wycofanie produktu lub usługi do którego/której mają zastosowanie postanowienia Regulaminu,
 - b. wprowadzenie przez Bank nowych produktów lub usług, do których będą miały zastosowanie postanowienia Regulaminu;
 - c. zmiana systemów informatycznych wykorzystywanych do obsługi oferowanych przez Bank produktów i usług, do których mają zastosowanie postanowienia Regulaminu;
 - d. zmiana przepisów prawa:
 - 1) regulujących produkty lub usługi oferowane przez Bank; do których zastosowanie mają postanowienia Regulaminu
 - 2) mających wpływ na wykonywanie Umowy lub Regulaminu;
 - e. zmiana lub wydanie nowych orzeczeń sądowych, orzeczeń organów administracji, zaleceń lub rekomendacji uprawnionych organów, w tym Komisji Nadzoru Finansowego – w zakresie związanym z wykonywaniem umowy lub Regulaminu.
2. W przypadku zmiany Regulaminu, Bank dostarczy Użytkownikowi tekst jednolity Regulaminu. Regulamin lub zmiany do Regulaminu dostarczane będą wyłącznie drogą elektroniczną (za pośrednictwem stron internetowych Banku, Bankowości Internetowej lub poczty email) nie później niż 2 miesiące przed proponowaną datą ich wejścia w życie. Brak zgłoszenia sprzeciwu Użytkownika wobec proponowanych zmian jest równoznaczny z wyrażeniem na nie zgody.
3. Regulamin dostarczony w sposób opisany w ust. 2 uznaje się za doręczony.
4. Użytkownik ma prawo, przed datą proponowanego wejścia w życie zmian, wypowiedzieć Umowę ze skutkiem natychmiastowym bez ponoszenia opłat związanych z wypowiedzeniem Umowy lub opłat wynikających z proponowanych zmian.
5. W przypadku gdy Użytkownik zgłosi sprzeciw zgodnie z ust. 2, ale nie dokona wypowiedzenia Umowy, Umowa

wygasza z dniem poprzedzającym dzień wejścia w życie proponowanych zmian, bez ponoszenia opłat związanych z wypowiedzeniem umowy lub opłat wynikających z proponowanych zmian.

§36

Bank zastrzega sobie prawo wykonywania niektórych usług w ramach Kanałów Elektronicznych za pośrednictwem podmiotów zewnętrznych, w szczególności podmiotów zależnych. Przekazywane do tych podmiotów dane objęte są tajemnicą bankową oraz postanowieniami ustawy o ochronie danych osobowych i podlegają ochronie w takim samym stopniu i zakresie jak w przypadku Banku. Bank ponosi pełną odpowiedzialność za transakcje wykonywane za pośrednictwem tych podmiotów.